

Bridging Security Intelligence: Hacking, Threat Hunting, AI, Behavioral Anomalies, and Incident Response



Michael Melore, CISSP

IBM Cyber Security Advisor



@MichaelMelore



Dangerous Toys

USB Device Impersonators

USB Killers

Man in the Middle Faceplates

Wireless Pineapples

Payload Phone Chargers



Dangerous Toys

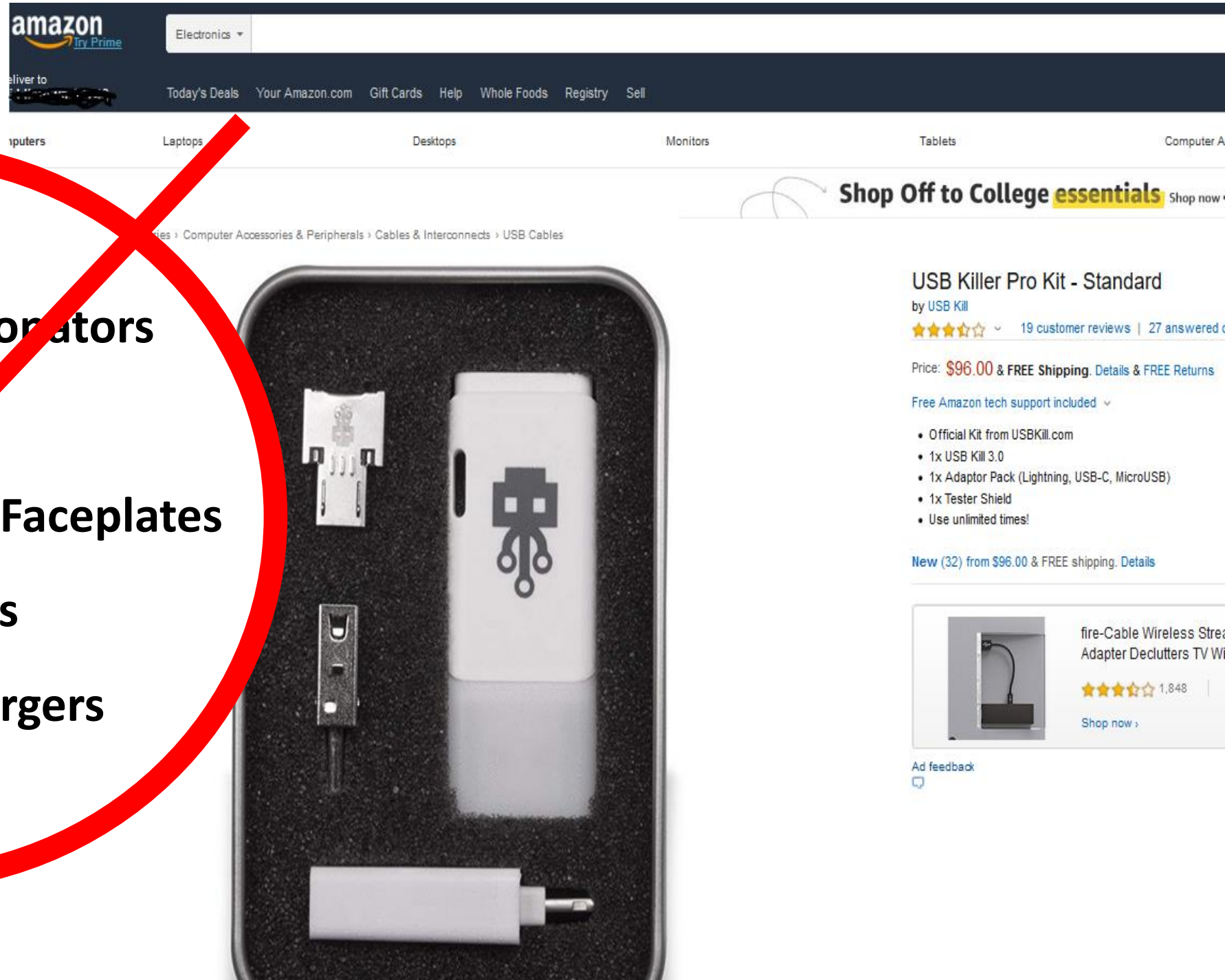
USB Device Impersonators

USB Killers

Man in the Middle Faceplates

Wireless Pineapples

Payload Phone Chargers



Dangerous Toys

USB Device Impersonators

USB Killers

Man in the Middle Faceplates

Wireless Pineapples

Payload Phone Chargers



[Wifi Pineapple Wireless Network Wifipineapple Wireless Security](#)

\$75.99 from eBay - chunyu1991_1

NOTE: The version of the **wireless** security auditing device wifipineapple sixth generation



[Wifi Pineapple Wireless Network Wifipineapple Wireless Security](#)

\$75.09 from eBay

WiFi Pineapple Wireless Network wifipineapple **wireless** security auditing hak5 Descrip
Wireless · USB · Wi-Fi



[Wifi Pineapple Wireless Network Security Audit Wireless Wifi Security](#)

\$62.69 from eBay - xiaof12

Please do not upgrade the new system firmware. If there is any problem, please brush bar
Wireless · 802.11n · 802.11g · 802.11b · USB · PC · Wi-Fi



[Lusya WiFi Pineapple Wireless Network Security Audit Wireless WIFI](#)

\$83.44 from AliExpress.com

in from on AliExpress.com | Alibaba Group

With Wi-Fi · Wireless

Dangerous Toys

USB Device Impersonators

USB Killers

Man in the Middle Faceplates

Wireless Pineapples

Payload Phone Chargers



Dangerous Toys

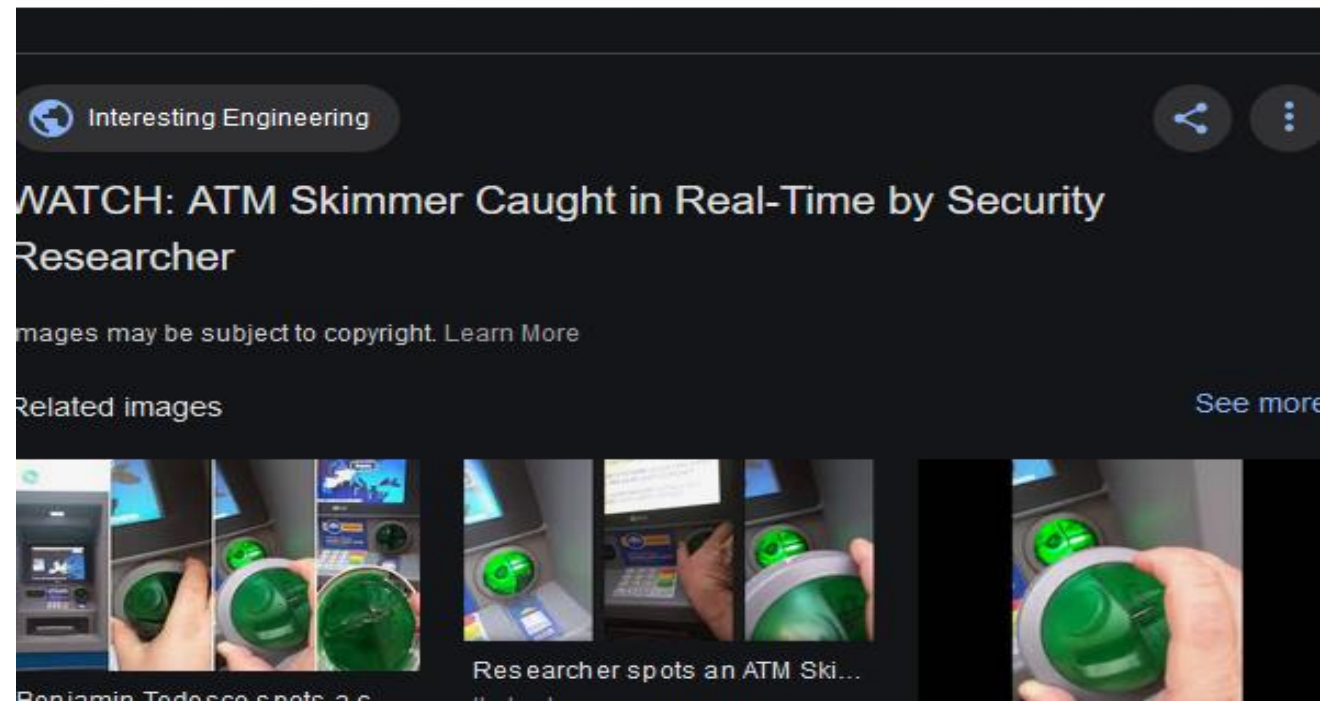
USB Device Impersonators

USB Killers

Man in the Middle Faceplates

Wireless Pineapples

Payload Phone Chargers





https://censys.io



FTP and Telnet Sites North Carolina US

[66.207.227.71 \(pode.intrstar.net\)](#)

☁ STARWIRELESS-15153 - StarVision, Inc. (15153) 📍 Dunn, North Carolina, United States
⚙️ 21/ftp, 23/telnet
🔍 location.province: North Carolina

[152.13.178.2 \(CAM225DSJ1300.uncg.edu\)](#)

☁ UNC-GREENSBORO - University of North Carolina at Greensboro (53785) 📍 Greensboro, North Carolina, United States
⚙️ 21/ftp, 23/telnet, 443/https, 80/http
🔒 HP Designjet 36B634A0
🔍 tags: ftp

[198.85.198.4](#)

☁ NCREN - MCNC (81) 📍 Albemarle, North Carolina, United States
⚙️ 21/ftp, 23/telnet
🔍 21.ftp.banner.banner: 220 Welcome to the Valere FTP server.

[152.20.39.207](#)

☁ NCREN - MCNC (81) 📍 Wilmington, North Carolina, United States
⚙️ 21/ftp, 23/telnet
🔍 21.ftp.banner.banner: 220 FTP print

[98.26.91.139 \(cpe-98-26-91-139.nc.res.rr.com\)](#)

☁ TWC-11426-CAROLINAS - Charter Communications Inc (11426) 📍 Durham, North Carolina, United States
⚙️ 21/ftp, 23/telnet
🔍 21.ftp.banner.banner: (VxWorks 5.5.1) FTP server ready



location.country_code: US and tags: scada

[64.19.73.45 \(45-73-19-64-wtn-ny.a-315.westelcom.com\)](#)

☁ WFC-ASN - Westelcom Internet, Inc. (11722) 📍 Watertown, New York, United States
🏢 Schneider Electric BMX P34 2020 v2.0 ⚙️ 502/modbus
🔍 tags: scada gateway
SCADA SCADA GATEWAY

[66.44.215.170 \(170.subnet-66-44-215.ellijay.com\)](#)

☁ ELJY30540 - Ellijay Telephone Company (25853) 📍 Blue Ridge, Georgia, United States
🏢 Schneider Electric BMX NOE 0100 V2.80 ⚙️ 502/modbus
🔍 tags: scada gateway
SCADA SCADA GATEWAY

[162.155.7.242 \(rrcs-162-155-7-242.central.biz.rr.com\)](#)

☁ TWC-10796-MIDWEST - Charter Communications Inc (10796) 📍 Strongsville, Ohio, United States
🏢 Schneider Electric BMX P34 2020 v2.5 ⚙️ 502/modbus
🔍 tags: scada gateway
SCADA SCADA GATEWAY

[166.250.100.120 \(120.sub-166-250-100.myvzw.com\)](#)

☁ CELLCO - Cellco Partnership DBA Verizon Wireless (22394) 📍 United States
🏢 Schneider Electric BMX P34 2020 v2.6 ⚙️ 502/modbus
🔍 tags: scada gateway
SCADA SCADA GATEWAY

https://shodan.io

Jo-ann Stores, LLC
Added on 2019-08-01 12:53:58 GMT
United States, Stow

166.215.52.198
mobile-166-215-52-198.mycingular.net
AT&T Wireless
Added on 2019-08-01 12:43:45 GMT
United States

ICS

209.201.40.202
209-201-40-202.dia.static.centurylink.net
CenturyLink
Added on 2019-08-01 12:44:05 GMT
United States, Logan

HTTP/1.1 400 Bad Request\r\nContent-Type: text/html; charset=us-ascii\r\nServer: Microsoft-HTTPAPI/2.0\r\nDate: Tl
\n<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"\"http://www.w3.org/TR/html4/strict.dtd">\r\n<HTML><HEAD...

67.141.196.22
h22.196.141.67.static.ip.windstream.net
Windstream Communications
Added on 2019-08-01 12:50:53 GMT
United States, Cornelius

ICS

165.227.224.226
Digital Ocean
Added on 2019-08-01 12:45:03 GMT
United States, New York

honeypot cloud

Basic Hardware: 6ES7 212-1BE31-0XB0 v.0.2
Module: 6ES7 212-1BE31-0XB0 v.0.2
Basic Firmware: 6ES7 212-1BE31-0XB0 v.3.0.2

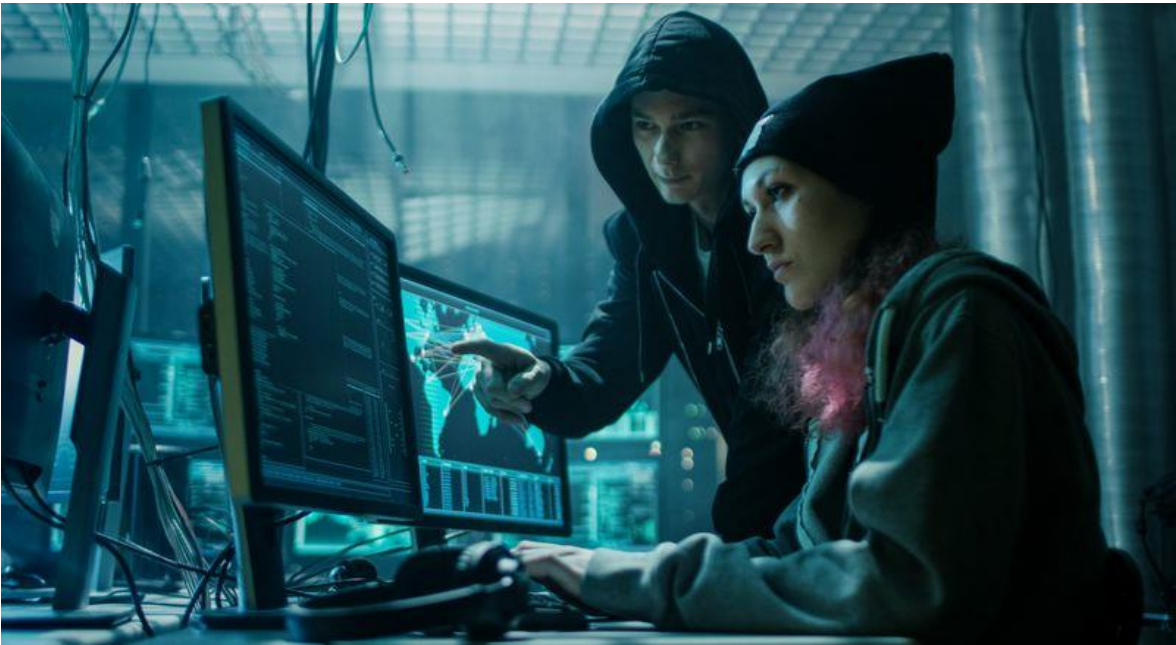
Basic Hardware: 6ES7 215-1HG31-0XB0 v.0.1
Module: 6ES7 215-1HG31-0XB0 v.0.1
Basic Firmware: 6ES7 215-1HG31-0XB0 v.3.0.2

Location designation of a module:
Copyright: Operation
Module type: IM151-8 PN/DP CPU
PLC name: Technodrome
Module: v.0.0
Plant identification: Mouser Factory
OEM ID of a module:
Module name: Operation
Serial number of module: 88111222

Basic Hardware: 6ES7 212-1BE31-0XB0 v.0.2

Module: 6ES7 212-1BE31-0XB0 v.0.2

Basic Firmware: 6ES7 212-1BE31-0XB0 v.3.0.2



https://haveibeenpwned.com

[Home](#)[Notify me](#)[Domain search](#)[Who's been pwned](#)[Passwords](#)[API](#)[About](#)[Donate !\[\]\(6059a5aa8b4ca7bb793408023d6c6e42_img.jpg\) !\[\]\(d293b9aef7d8767760396289fbc64e8a_img.jpg\)](#)

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

pwned?



Generate secure, unique passwords for every account

[Learn more at 1Password.com](#)

[Why 1Password?](#)

363

pwned websites

7,858,185,878

pwned accounts

94,865

pastes

116,710,196

paste accounts

<http://informationisbeautiful.net>

information is beautiful

[home](#) [about](#) [blog](#) [data](#) [training](#) [books](#) [contact](#)

[f](#) [t](#) [in](#) [rss](#) [envelope icon](#) [search icon](#)

Learn the art of data visualization
Our next London workshop is on 13th March 2019

[Book Now](#)

What could really increase your life expectancy, lifespan and longevity?



Brexit Visual Video Explainer



WDVP Gallery 2019



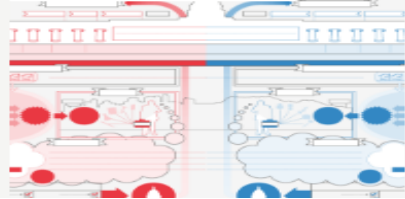
Because Every Country Is the Best at Something



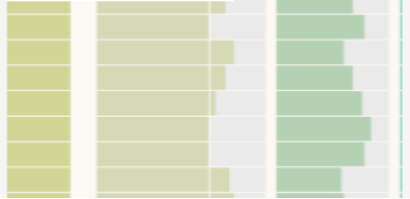
Best in Show - What's the Best Dog Breed, According to Data?



Left vs Right (World)



Diversity in Tech



Intermental



http://informationisbeautiful.net

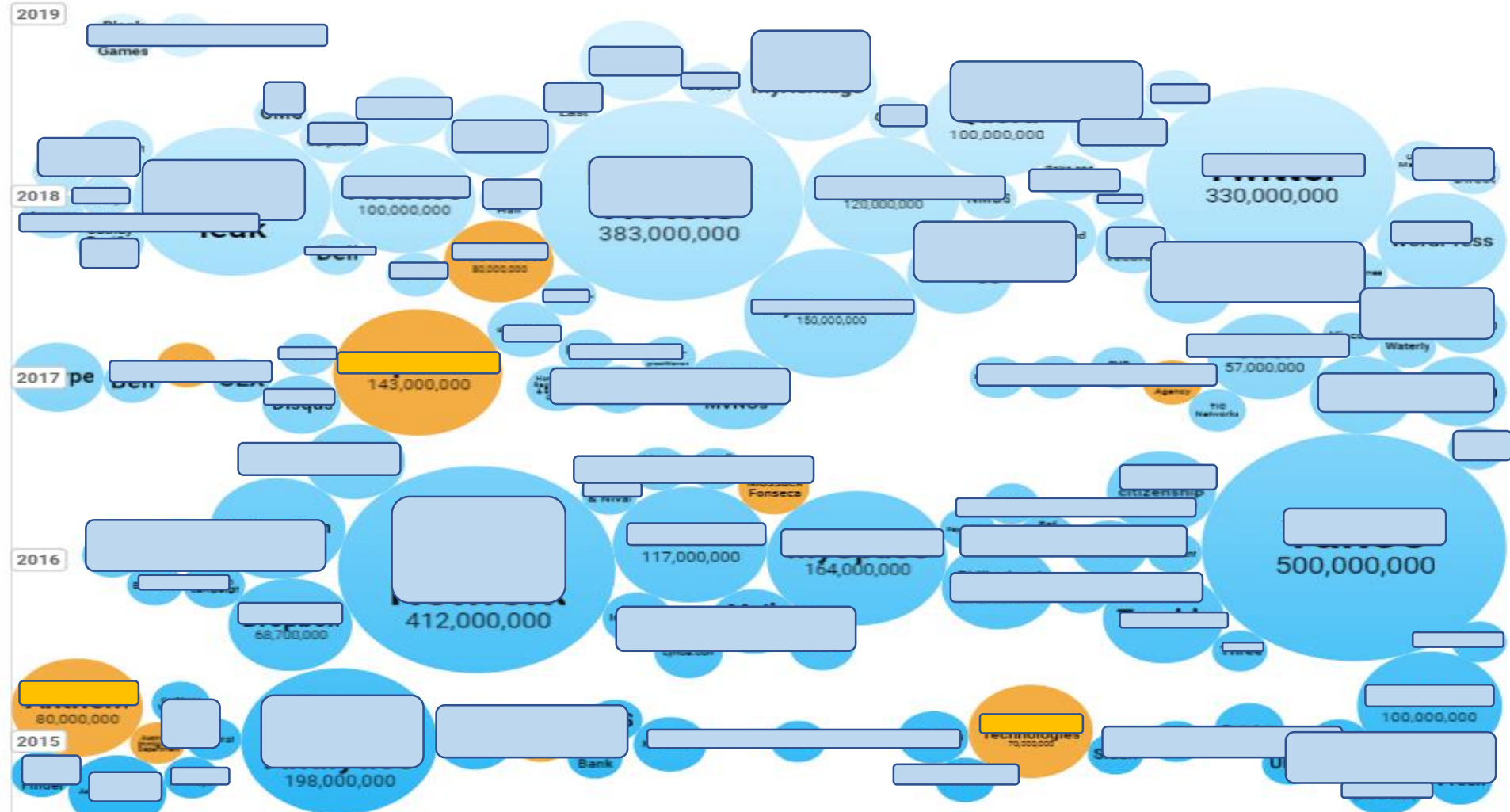
World's Biggest Data Breaches & Hacks

Select losses greater than 30,000 records
(updated 1st Feb 2019)

Colour YEAR DATA SENSITIVITY Filter

Search...

Interesting
Story



The Song Remains The Same

- Defense in depth failures
- Average separate security solutions
- Time to discover Breaches
- Time to respond to Incidents
- Cost of a breach

Since 1984 and still not effective

40+ (30% feel right number)

200 Days

56 Days

\$3.9 Million



State Sponsored
Actors

Sophisticated
Talent

Anonymous
Digital Currencies

Highly Funded
R&D

Collaborative
Development

Circumventive
Tooling

Organized Threat Actors



Crowd-sourced information sharing

Threats Du Jour

Start your 30-day trial

[View API documentation](#)



Groups

Focal point for collaboration and sharing



Security-Analyst

354 Members | 7 Collections



Feedback - IBM X-Force Exchange

289 Members | 4 Collections

[Manage Groups](#)



Threat Activity

Malicious IP addresses in the last hour

Total	369
Command and Control	3
Spam	188
Malware	0
Scanning	190

[View threat activity map](#)



Security Intelligence Blog

Analysis and insight on information security, by IBM

10 Do's and Don'ts for Writing a Winning Cybersecurity Resume

Oct 4, 2019 - By Jasmine Henry

When Digital Identity and Access Management Meets Physical Security

Oct 3, 2019 - By George Platiss

Ramnit Targets Japanese Shoppers, Aiming at Top Fashion Brands

Oct 3, 2019 - By Itzik Chimino

[Visit Security Intelligence Blog](#)

Start your 30-day trial

[Visit Early Warning dashboard](#)



Public Collections

Publicly shared community findings

Recommended



Botnet Command and Control Servers

Oct 3, 2019 - x-force



Malware hashes

Sep 26, 2019 - test, malware



STIX 2.1 Update

Sep 25, 2019 - stix, taxii



The Massive Propagation of the Smominru Botnet

Sep 23, 2019 - advisory, botnet, malware, xfas

Most Recent



XFTAS Daily Threat Assessment for October 03, 2019

Oct 4, 2019 - xftas



Botnet Command and Control Servers

Oct 3, 2019 - x-force



XFTAS Daily Threat Assessment for October 02, 2019

Oct 3, 2019 - xftas



Phishing

Oct 3, 2019

[View more](#)



Featured from App Exchange

Verified extensions for a stronger enterprise defense



QRadar Advisor With Watson

IBM QRadar

Enrich security incidents with insights from Watson to rapidly respond to threats.

[View more](#)

Start your 30-day trial

Premium IRIS Threat Reports



Travel Agencies and Services Industry Profile

Last Updated : Jul 15, 2019



Oil & Gas Industry Profile

Last Updated : Jul 15, 2019



NewCT Analysis Report

Last Updated : Jul 15, 2019



CobaltStrike Loader and Payload Analysis Report

Last Updated : Jul 15, 2019



Hive0045 Analysis Report

Last Updated : Jul 14, 2019

[Unlock all IRIS reports](#)



My Collections

Use Collections to store and share your findings

You did not create any Collections yet.

Recently shared with me



Spam campaign delivers Malware

Aug 1, 2018



BadRabbit Malware

Oct 26, 2017 - backdoor, ransomware, exploit-kit, threat-re...

[View more](#)



Botnet Distribution

azorult



Affected Countries

115

Peak

Sep 18, 2019

Trend



[View more](#)

Oct 4, 2019

[View more](#)



Vulnerabilities

The latest global security risks



HHVM number_format code execution

Consequences: Gain Access



WhatsApp App for Android DDGifSlurp function code execution

Consequences: Gain Access



Micro Focus Enterprise Developer and Enterprise Server cross-site scripting

Consequences: Cross-Site Scripting



Node.js realms-shim module code execution

Consequences: Gain Access



Node.js realms-shim module code execution

Consequences: Gain Access



Ubercart module for Drupal cross-site scripting

Consequences: Cross-Site Scripting



Simple AMP module for Drupal security bypass

Consequences: Bypass Security

[View more](#)



IBM X-Force Commercial API

Programmatic access to the IBM X-Force Exchange



Query our threat intelligence through a RESTful API that supports multiple formats (including JSON and STIX/TAXII) for a simple integration with your security tools.

[Start your 30-day trial](#)

[View API Documentation](#)

Training Exercises



Protect your information, contain the risk

Identify risks

- Discover, classify business critical data and apps
- Expose over privileges with identity analytics
- Analyze cloud app usage and activity
- Detect web fraud with real time alerts

Gain control

- Govern all users and their privileges
- Protect data usage across enterprise and cloud
- Improve DevOps security
- Secure mobile devices and apps

Safeguard interactions

- Deploy adaptive access and web app protection
- Federate to and from the cloud
- Maintain data compliance and stop attacks
- Secure mobile collaboration

Who are High Performers?

Represent 26% of the 3655
in the study

Highest level of cyber resilience

More prepared to respond

Less impacted by cyber threats.

Report less attacks, better containment and
recovery



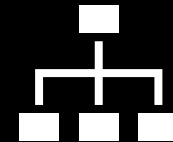
Confidence



Dedication



Communication
Skills



Industry Awareness

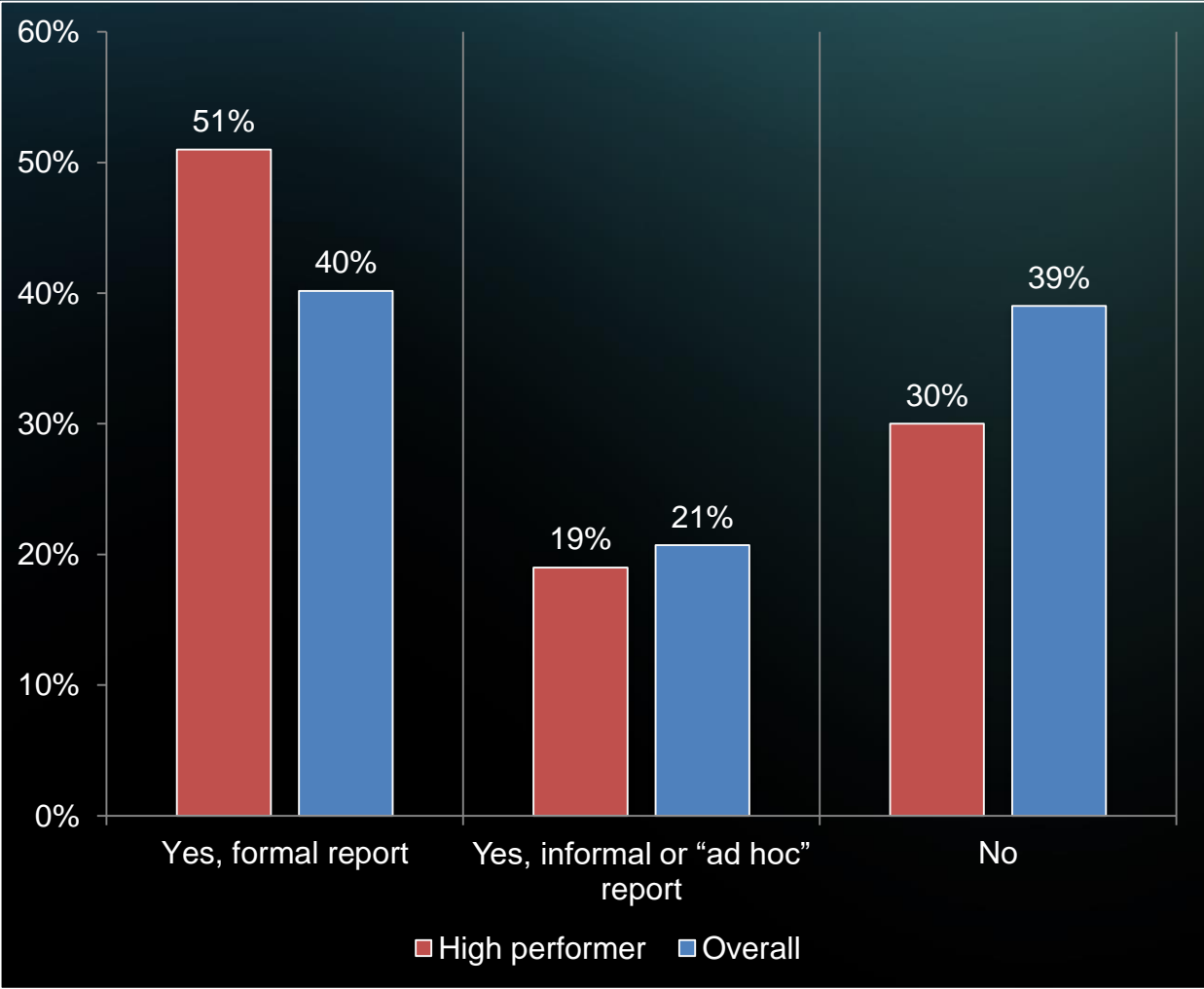


Streamlined SOC

High Performers Talk to the Board & C Suite Regularly

70%

produce either a formal or
'ad hoc' report on the
organizations Cyber
Resilience to their executive
level and Board



Workflow



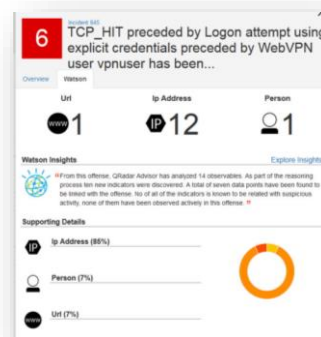
Advanced Analytics



DETECT



Cognitive



ENRICH



Threat Hunting



INVESTIGATE



ORCHESTRATE



Incident Response



User Behavior

Dashboard

Search For User

Q

Next Refresh: 00:09

Reset Layout

Monitored Users

401

Current High Risk Users

3

Sense Events (Last Hour)

42

Offenses Generated (Last Hour)

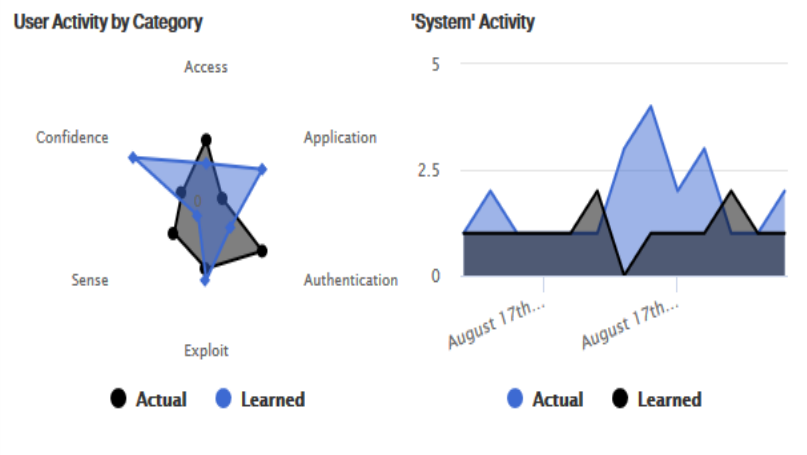
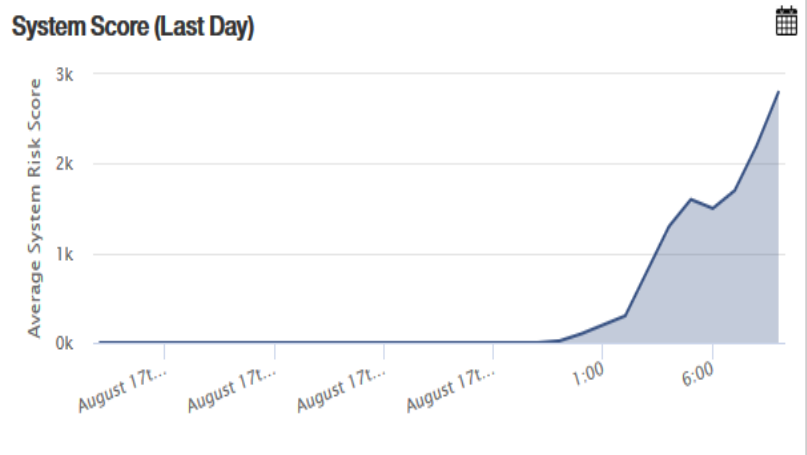
0

Active Insights

- Event Rules

Flow Rules
- Anomaly Detection Rules

Machine Learning Algorithms



Recent Offenses

Offense #90

about 2 hours ago

User: Mary Arnold

Event Count: 43

Flow Count: 0

Magnitude: 3/10

Offense #91

about 2 hours ago

User: Nathan Farrell

Event Count: 38

Flow Count: 8

Magnitude: 5/10

Offense #92

about 2 hours ago

User: Craig Murphy

Event Count: 38

Flow Count: 8

Magnitude: 5/10

Offense #97

about 2 hours ago

User: tom_wilson

Event Count: 43

Flow Count: 0

Magnitude: 3/10

Risky Users (Overall Score)

[View All](#)

	Mary Arnold	2891	👁
	Nathan Farrell	2291	👁
	Craig Murphy	1826	👁
	tom_wilson	1436	👁
	adam.benett	0	👁
	admin	0	👁

Most Suspicious Users (Window Score)

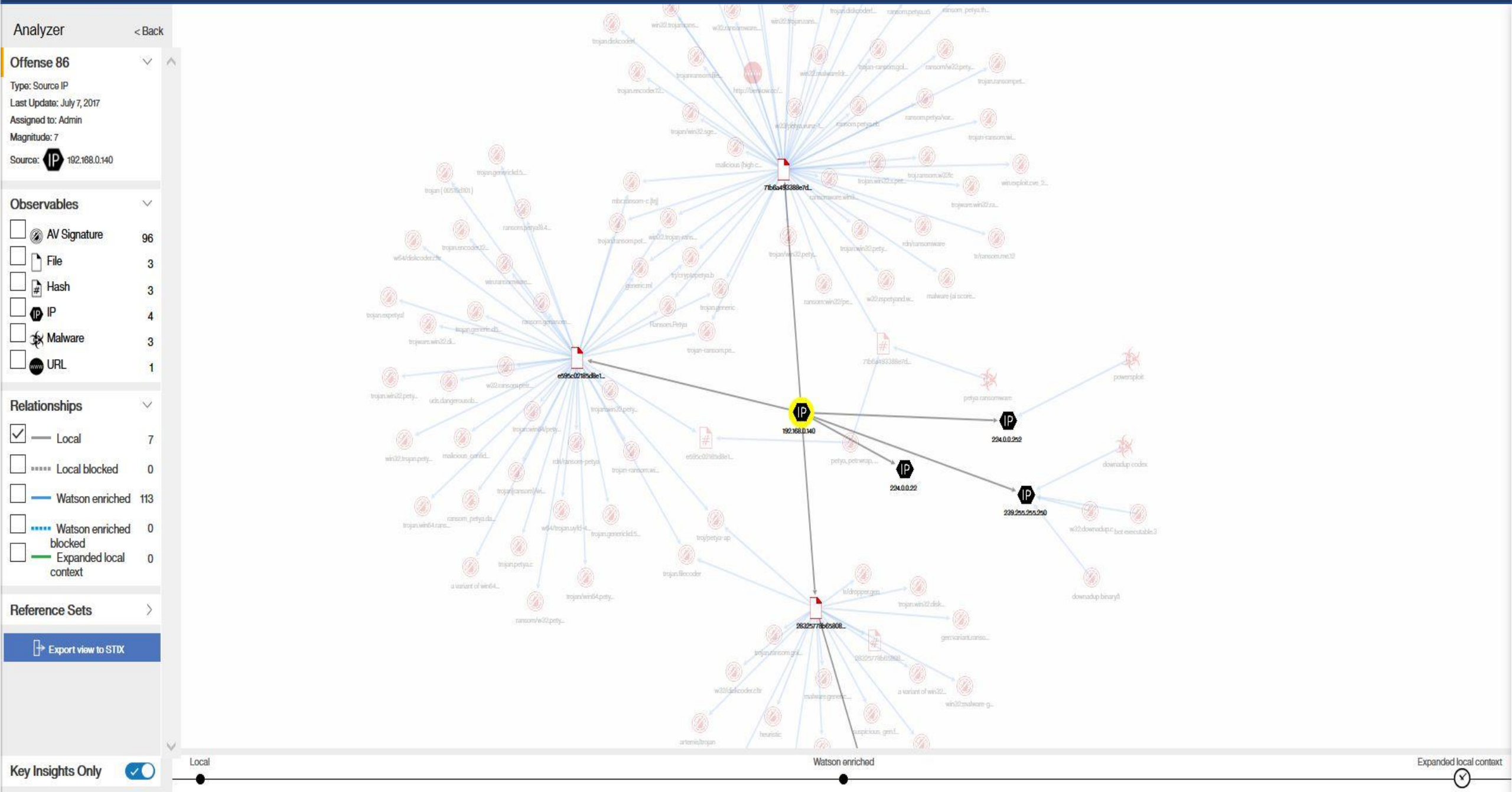
[View All](#)

	Mary Arnold	+2891	👁
	Nathan Farrell	+2291	👁
	Craig Murphy	+1826	👁
	tom_wilson	+1436	👁
	adam.benett	+0	👁
	admin	+0	👁

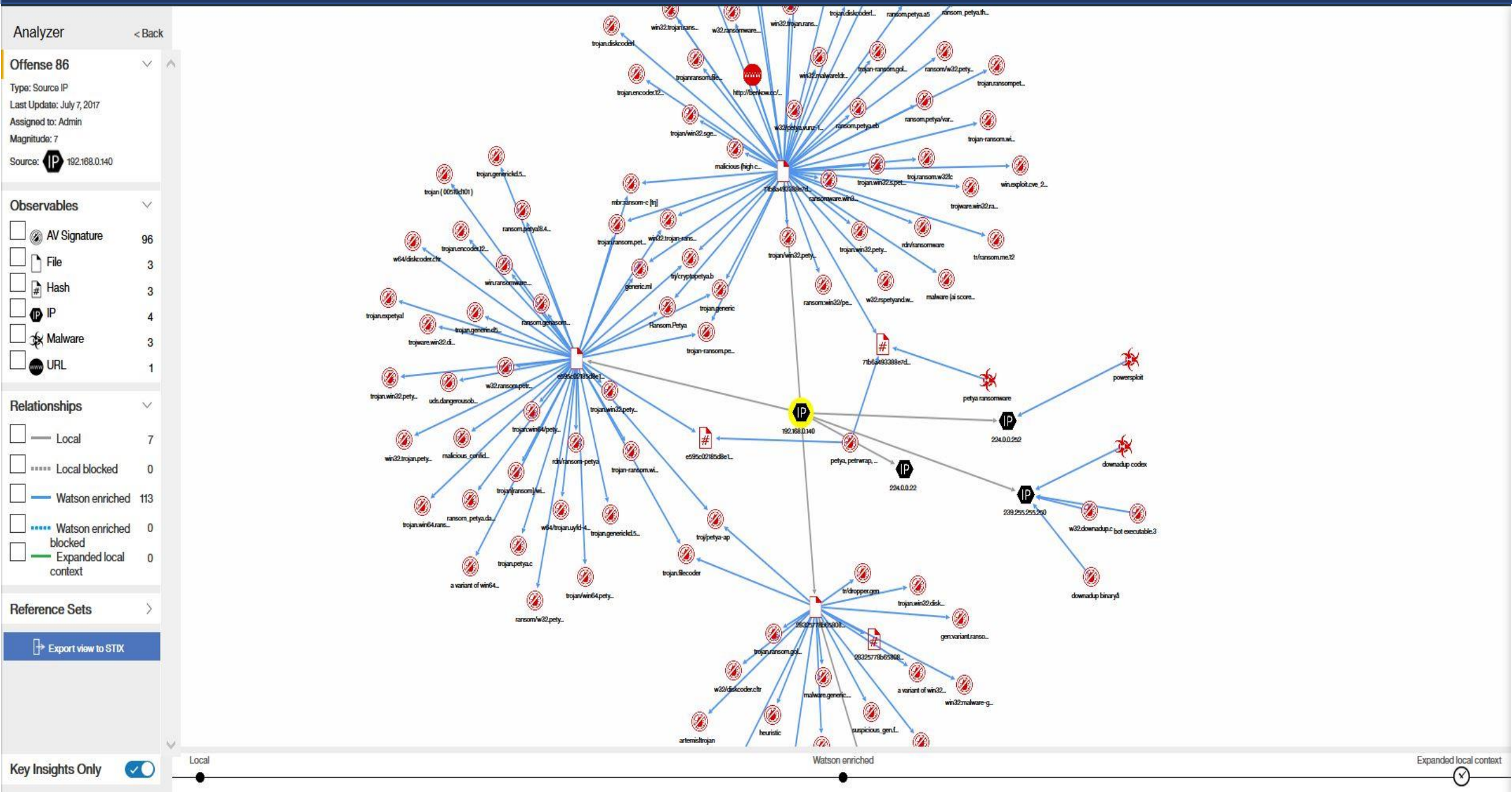
Watchlist

Mary Arnold	2891	📈	⊖
Nathan Farrell	2291	📈	⊖
Craig Murphy	1826	📈	⊖

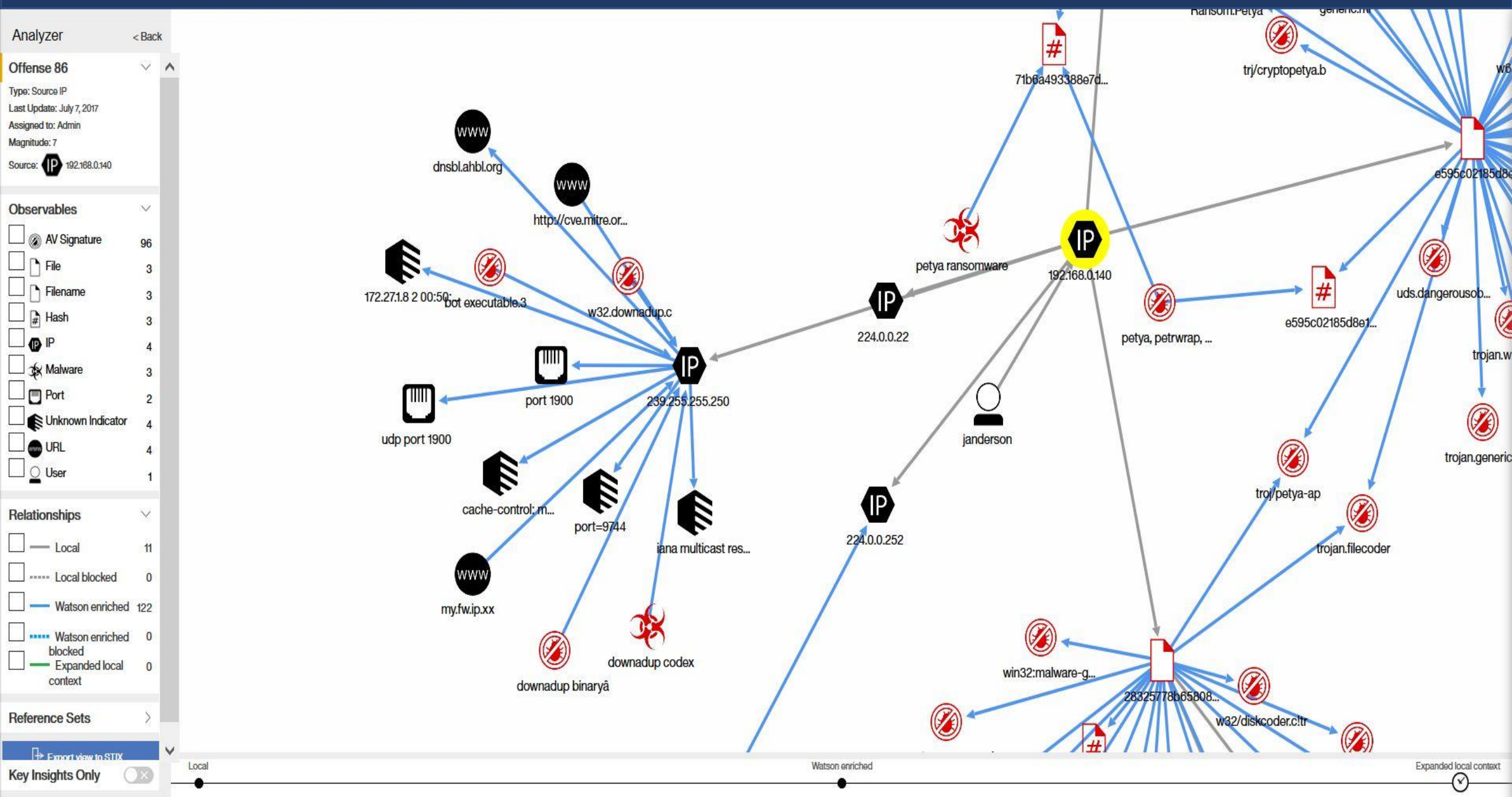
Local Analysis



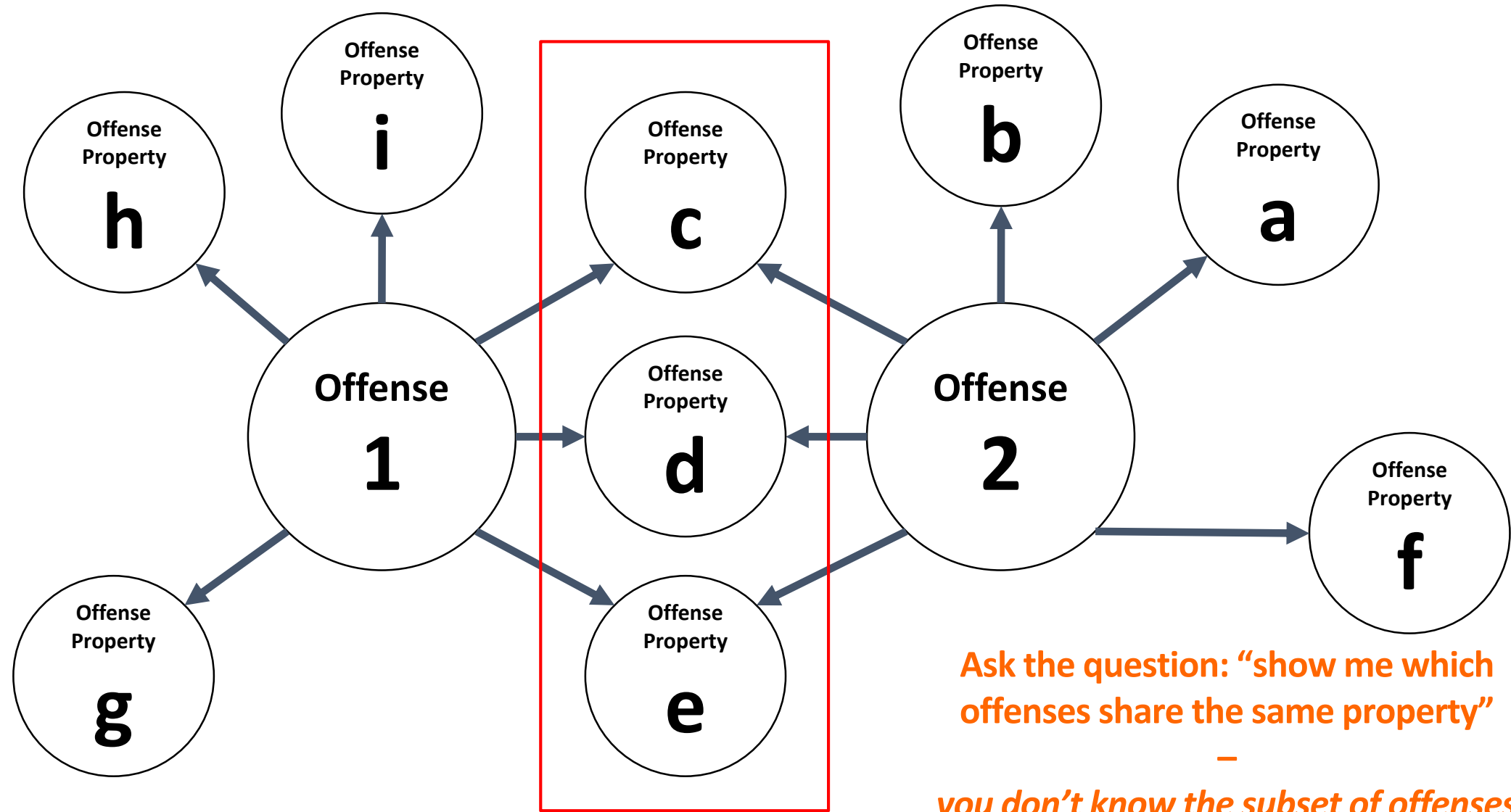
AI Enriched Analysis



AI Deep Insight



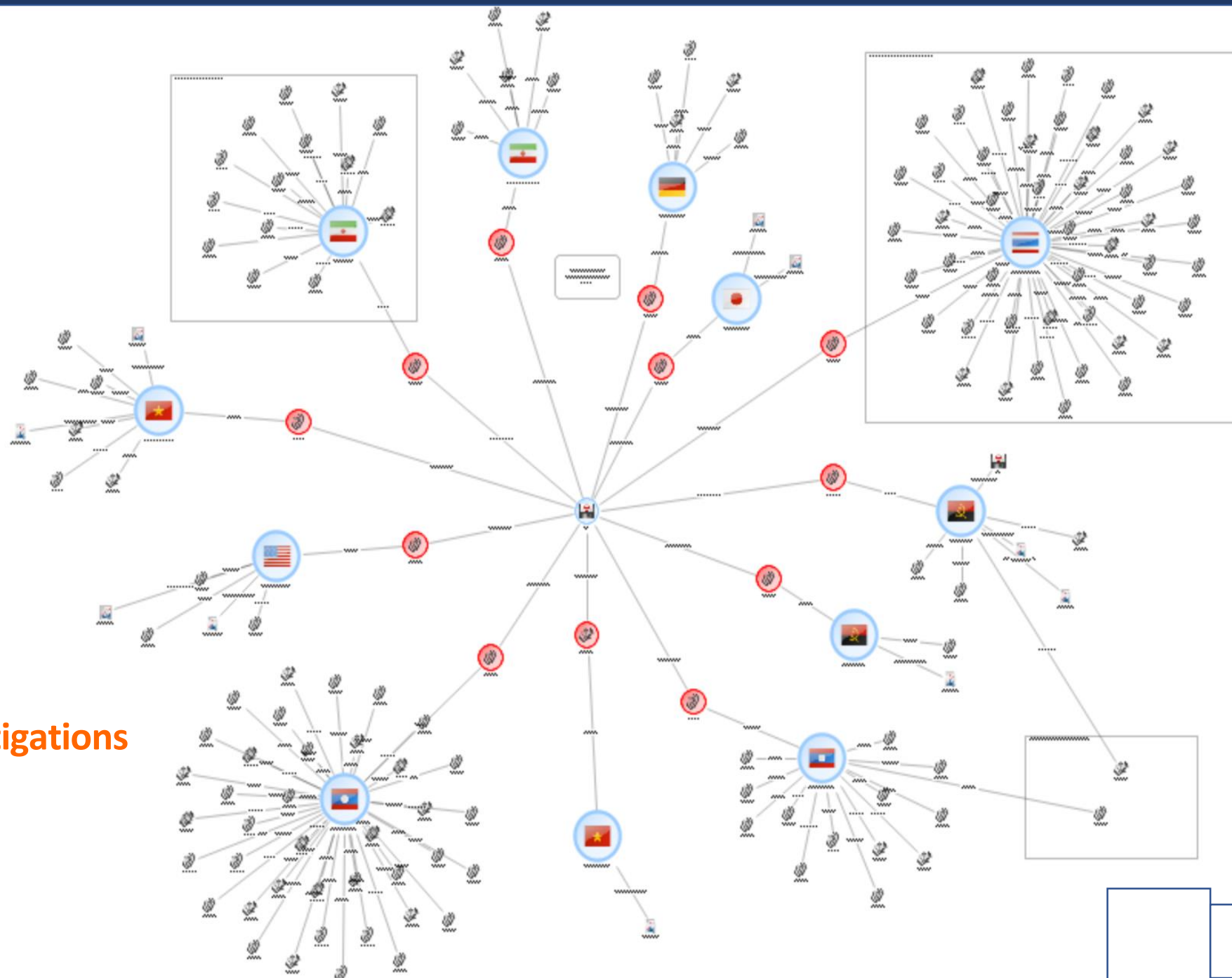
What is an Unknown Unknown Search



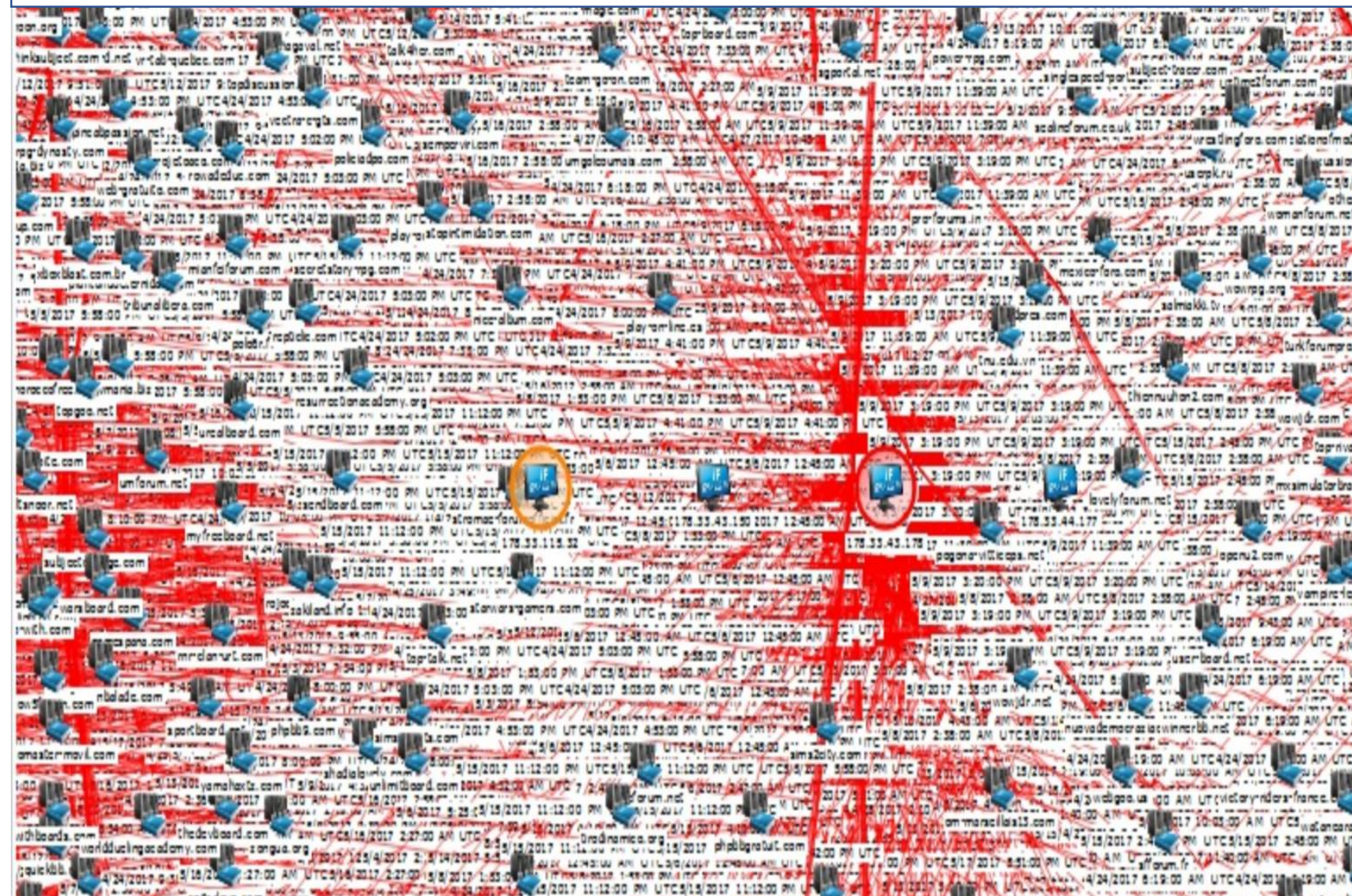
Ask the question: "show me which offenses share the same property"

—
you don't know the subset of offenses,
not the subset of properties to search

Investigations



Threat Hunting



Counts Values

The number of links or number of connected items are counted

Most links

Most inbound

Connections with the most links

Restrict

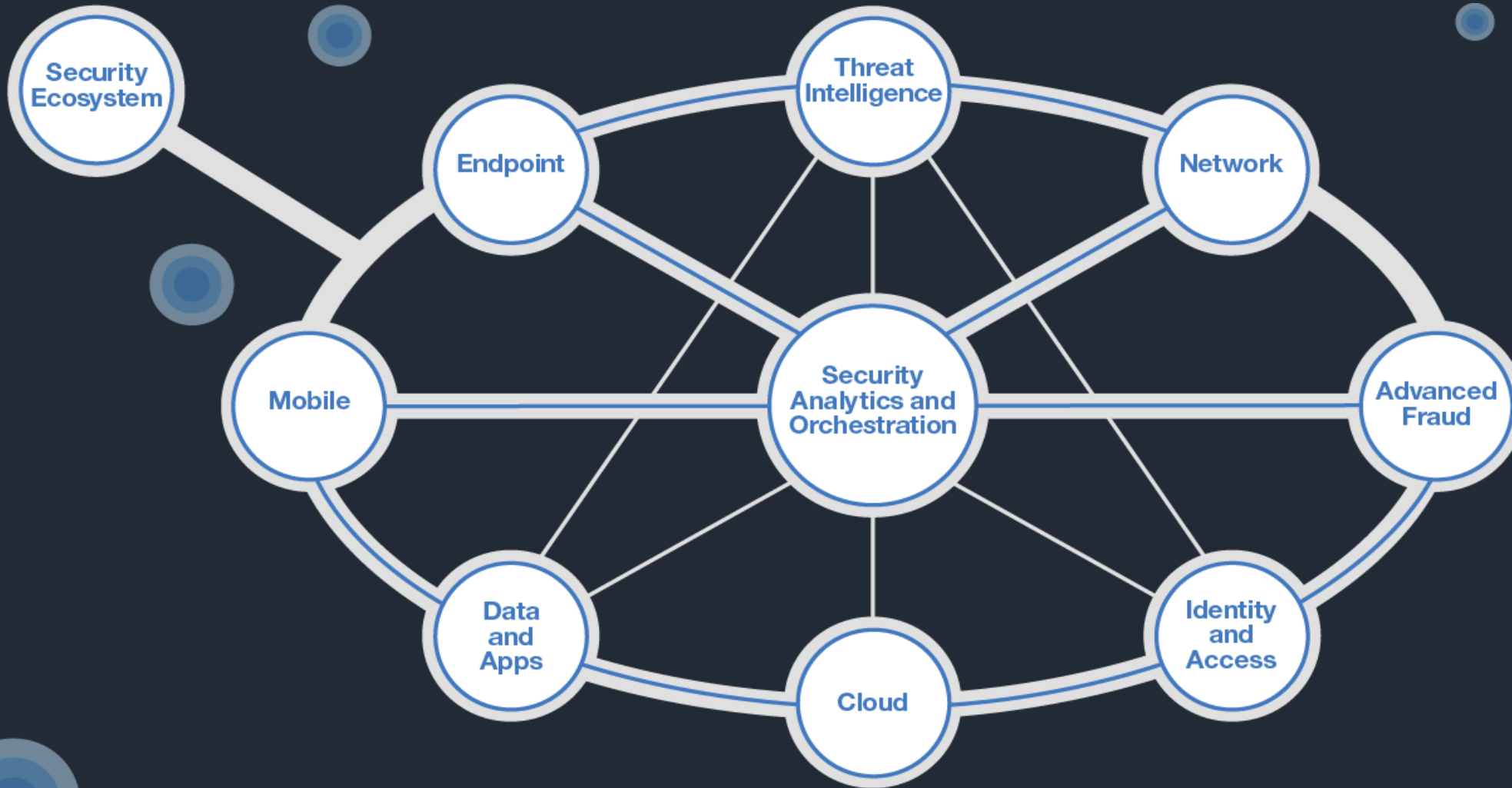
Entities with the most links

50%				
178.33.43.178	14571			
178.33.115.32	4927			
178.33.44.177	4914			
178.33.43.150	4863			

Incident Response Platform



Integrated and Intelligent Controls





Bridging Security Intelligence: Hacking, Threat Hunting, AI, Behavioral Anomalies, and Incident Response

Michael Melore, CISSP
IBM Cyber Security Advisor



@MichaelMelore

